UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,929	10/13/2004	Rajnish K. Chitkara	SYB/0110.01	5928

31779 7590 09/10/2009

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

EXAMINER	
GORTAYO, DANGELINO N	
ART UNIT	PAPER NUMBER
2168	

MAIL DATE	DELIVERY MODE
09/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/711,929	CHITKARA ET AL.	
	Examiner	Art Unit	
	DANGELINO N. GORTAYO	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-99* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-99* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/15/2009 has been entered.

Response to Amendment

2. In the amendment filed on 6/15/2009, claims 1, 4-6, 8-9, 32, 37, 41-42, 4452-53, 56, 64-67, 71, 74, 80, 88, 90, 92-97 have been amended. The currently pending claims considered below are Claims 1-99.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-31, 36-65, 70-73, and 78-99 are rejected under 35 U.S.C. 102(e) as being unpatentable over He et al. (US Patent 7,269,729 B2).

As per claim 1, He teaches "In a database system, a method for providing automated encryption support for column data," (see Abstract)

"the method comprising: defining Structured Query Language (SQL) extensions for creating and managing column encryption keys, and for creating and managing database tables with encrypted column data;" (column 1 lines 60-67, column 3 lines 17-57, column 4 lines 1-57, wherein a security catalog is utilized by extended SQL syntax statements to access a secure database)

"receiving a first SQL statement employing said SQL extensions to create a named encryption key for encrypting column data;" (column 6 line 39 – column 7 line 55, wherein public encryption keys are created for encrypting column data)

"parsing the first SQL statement, including creating said named encryption key with a syntactically unique name that can be parsed from within other SQL statements employing said SQL extensions;" (column 6 line 39 – column 7 line 22, column 8 lines 2-44, wherein a public key can be utilized to be employed by SQL statements)

"receiving a second SQL statement employing said SQL extensions to create a database table having particular column data encrypted with said named encryption key;" (column 5 lines 6-33, column 8 lines 2-45, wherein an SQL statement to create database tables with particular column data encrypted with an encryption key is received)

"parsing the second SQL statement, including identifying said named encryption key upon parsing a portion of the statement that comprises the syntactically unique name for the key;" (column 8 line 2 - column 9 line 17, wherein the SQL statement to create a table is parsed and the encryption key related to the column is identified)

"in response to parsing the second SQL statement, creating a database table having particular column data encrypted with said named encryption key identified upon parsing the second SQL statement;" (column 5 lines 5-33, column 8 line 2 - column 9 line 17, wherein the database table with encrypted column data is created)

"and in response to a subsequent database operation that requires particular column data that has been encrypted with said named encryption key, automatically decrypting the particular column data with said named encryption key, so that the particular column data is available in decrypted form for use by the database operation." (column 7 line 42-7, column 8 lines 25-44, column 9 lines 13-37, wherein the encrypted column data can be dynamically decrypted based on key access, to be used in database operation)

As per claim 2, He teaches "columns that are not specified to be encrypted are stored in unencrypted format, for minimizing encryption overhead." (column 5 lines 6-39)

As per claim 3, He teaches "the automated encryption support operates as an internal built-in feature of the database system, without use of an add-on library." (column 2 line 66 – column 3 line 6)

As per claim 4, He teaches said first SQL statement employing said SQL extensions to create a named encryption key is received from a user serving as a system security officer. (column 4 lines 1-33)

As per claim 5, He teaches "said second SQL statement employing said SQL extensions to create a database table having particular column data encrypted with said named encryption key may be received from a user other than the system security officer." (column 3 lines 17-45, column 4 lines 33-56)

As per claim 6, He teaches said first SQL statement employs an SQL extension having a CREATE ENCRYPTION KEY command. (column 6 line39 - column 7 line 55)

As per claim 7, He teaches the CREATE ENCRYPTION KEY command includes:

```
CREATE ENCRYPTION KEY keyname
[AS DEFAULT] [FOR algorithm]
[WITH [KEYLENGTH keysize]
[PASSWD passphrase]
[INIT_VECTOR [RANDOM | NULL]]
[PAD [RANDOM | NULL]]]
```

as its syntax. (column 6 line39 - column 7 line 55)

As per claim 8, He teaches said second SQL statement comprises a CREATE TABLE command that allows specification of one or more columns to be encrypted. (column 5 lines 6-38, column 8 lines 2-44)

As per claim 9, He teaches the CREATE TABLE command includes:

```
CREATE TABLE tablename
(colname1 datatype [encrypt [with [db.[owner].]keyname],
colname2 datatype [encrypt [with [db.[owner].]keyname])
```

as its syntax. (column 5 lines 6-38, column 8 lines 2-22)

As per claim 10, He teaches receiving an SQL statement specifying alteration of a previously-created database table so as to encrypt particular column data. (column 5 lines 32-64)

As per claim 11, He teaches the SQL statement specifying alteration of a previously created database table comprises an ALTER TABLE command. (column 5 lines 32-64)

As per claim 12, He teaches the ALTER TABLE command includes:

ALTER TABLE tablename MODIFY column_name
[[datatype] [null|not null]]
[decrypt | encrypt [with [db.[owner].]keyname]]

as its syntax. (column 5 lines 32-64)

As per claim 13, He teaches the encryption support works transparently with existing database applications.(column 9 line 61 – column 10 line 12)

As per claim 14, He teaches the database system includes a database server and one or more database clients, and wherein method steps implementing the encryption support are embodied at the database server. (column 3 lines 37-45)

As per claim 15, He teaches the database system includes a back-end server tier and a middleware tier, and wherein method steps implementing the encryption support are embodied at the back-end server tier. (column 3 lines 37-45)

As per claim 16, He teaches after creation of the named encryption key, protecting the named encryption key with a user-supplied password. (column 6 line 38 – column 7 line 22)

As per claim 17, He teaches the user-supplied password must be supplied before the system allows use of the named encryption key for database operations. (column 6 line 38 – column 7 line 22)

As per claim 18, He teaches the user-supplied password is supplied using a SET ENCRYPTION PASSWD command. (column 6 line 38 – column 7 line 22)

As per claim 19, He teaches the SET ENCRYPTION PASSWD command includes:

SET ENCRYPTION PASSWD password FOR keyname

as its syntax. (column 6 line 38 – column 7 line 22)

As per claim 20, He teaches a user seeking to decrypt column data must supply said user-supplied password and must have necessary database privileges before decrypting the column data with the named encryption key. (column 7 lines 36-55)

As per claim 21, He teaches the user-supplied password is supplied using a SET ENCRYPTION PASSWD command. (column 6 line 38 – column 7 line 22)

As per claim 22, He teaches providing a command to grant decryption permission to others. (column 8 line 46 – column 9 line 37)

As per claim 23, He teaches the command to grant decryption permission includes:

GRANT DECRYPT ON table.column TO user_or_role_list

as its syntax. (column 8 line 46 – column 9 line 37)

As per claim 24, He teaches the database system internally stores in encrypted format any column encryption keys that have been created. (column 3 lines 37-57, column 8 lines 38-44)

As per claim 25, He teaches the database system stores encrypted column data internally as variable binary (VARBINARY) data. (column 5 lines 18-64)

As per claim 26, He teaches the database system presents users a user-defined field type for column data that has been encrypted, even though the column data is stored internally as variable binary data. (column 5 lines 18-64)

As per claim 27, He teaches the database system preserves any user-defined data type for the particular column data so that the database system employs a correct data type for processing queries and returning query results. (column 3 lines 17-57)

As per claim 28, He teaches the database system stores the user-defined data type for the particular column data in a system catalog of the database system. (column 3 lines 17-57)

As per claim 29, He teaches the named encryption key created comprises a symmetric encryption key. (column 5 lines 18-64)

As per claim 30, He teaches a single column named encryption key is used for each column to be encrypted. (column 6 lines 18-37)

As per claim 31, He teaches a single column encryption key may be shared by multiple columns to be encrypted. (column 8 lines 25-44)

As per claim 36, He teaches said Structured Query Language (SQL) extensions for creating and managing named encryption keys include a clause for instructing the database system to create a default key for encrypting columns. (column 8 lines 2-24)

As per claim 37, He teaches "A database system providing automated encryption support for column data," (see Abstract)

"the system comprising: a processor" (column 3 lines 7-15)

"a memory coupled to the processor;" (column 3 lines 7-23)

"a parser that supports Structured Query Language (SQL) extensions for creating and managing named encryption keys for encrypting column data, and for creating and managing database tables with encrypted column data;" (column 1 lines 60-67, column 3 lines 17-57, column 4 lines 1-57, wherein a security catalog is utilized by extended SQL syntax statements to access a secure database)

"and an execution unit, operating in response to SQL statements parsed by the parser, that creates in response to parsing a first SQL statement employing said SQL extensions a particular named encryption key having syntactically unique name that can be parsed from within other SQL statements employing said SQL extensions," (column 6 line 39 – column 7 line 22, column 8 lines 2-44, wherein a public key can be created and employed by SQL statements)

"creates in response to parsing a second SQL statement employing said SQL extensions one or more database tables having particular column data encrypted with said particular named encryption key, including identifying said particular named

encryption key upon parsing a portion of the statement that comprises the syntactically unique name for the key," (column 5 lines 6-33, column 8 line 2 – column 9 line 17, wherein an SQL statement to create database tables with particular column data encrypted with an encryption key is received)

"and automatically decrypts the particular column data for use by a subsequent database operation that requires the particular column data that has been encrypted." (column 7 line 42-7, column 8 lines 25-44, column 9 lines 13-37, wherein the encrypted column data can be dynamically decrypted based on key access, to be used in database operation)

As per claim 38, He teaches columns that are not specified to be encrypted are stored in unencrypted format, for minimizing encryption overhead. (column 5 lines 6-39)

As per claim 39, He teaches the automated encryption support operates as an internal built-in feature of the database system, without use of an add-on library. (column 2 line 66 – column 3 line 6)

As per claim 40, He teaches said first SQL statement specifying creation of a particular named encryption key is received from a user serving as a system security officer. (column 4 lines 1-33)

As per claim 41, He teaches said second SQL statement specifying creation of one or more database tables may be received from a user other than the system security officer. (column 3 lines 17-45, column 4 lines 33-56)

As per claim 42, He teaches said first SQL statement specifying creation of a particular named encryption key comprises a CREATE ENCRYPTION KEY command. (column 6 line 39 - column 7 line 55)

As per claim 43, He teaches the CREATE ENCRYPTION KEY command includes:

CREATE ENCRYPTION KEY keyname
[AS DEFAULT] [FOR algorithm]
[WITH [KEYLENGTH keysize]
[PASSWD passphrase]
[INIT_VECTOR [RANDOM | NULL]]
[PAD [RANDOM | NULL]]]

as its syntax. (column 6 line 39 - column 7 line 55)

As per claim 44, He teaches said second SQL statement specifying creation of one or more database tables having particular column data encrypted comprises a CREATE TABLE command that allows specification of one or more columns to be encrypted. (column 5 lines 6-38, column 8 lines 2-44)

As per claim 45, He teaches the CREATE TABLE command includes:

CREATE TABLE tablename
(colname1 datatype [encrypt [with [db.[owner].]keyname],
colname2 datatype [encrypt [with [db.[owner].]keyname])

as its syntax. (column 5 lines 6-38, column 8 lines 2-44)

As per claim 46, He teaches a module for receiving an SQL statement specifying alteration of a previously created database table so as to encrypt particular column data. (column 5 lines 32-64)

As per claim 47, He teaches the SQL statement specifying alteration of a previously created database table comprises an ALTER TABLE command. (column 5 lines 32-64)

As per claim 48, He teaches the ALTER TABLE command includes:

ALTER TABLE tablename MODIFY column_name
[[datatype] [null|not null]]
[decrypt | encrypt [with [db.[owner].]keyname]]

as its syntax. (column 5 lines 32-64)

As per claim 49, He teaches the encryption support works transparently with existing database applications. (column 9 line 61 – column 10 line 12)

As per claim 50, He teaches the database system includes a database server and one or more database clients, and wherein the encryption support is provided by the database server. (column 3 lines 37-45)

As per claim 51, He teaches the database system includes a back-end server tier and a middleware tier, and wherein the encryption support is provided by the back-end server tier. (column 3 lines 37-45)

As per claim 52, He teaches the system protects the particular named encryption key with a user-supplied password. (column 6 line 38 – column 7 line 22)

As per claim 53, He teaches the user-supplied password must be supplied before the system allows use of the particular named encryption key for database operations. (column 6 line 38 – column 7 line 22)

As per claim 54, He teaches the user-supplied password is supplied using a SET ENCRYPTION PASSWD command. (column 6 line 38 – column 7 line 22)

As per claim 55, He teaches the SET ENCRYPTION PASSWD command includes:

SET ENCRYPTION PASSWD password FOR keyname

as its syntax. (column 6 line 38 – column 7 line 22)

As per claim 56, He teaches a user seeking to decrypt column data must supply said user-supplied password and must have necessary database privileges before decrypting the column data with the particular named encryption key. (column 7 lines 36-55)

As per claim 57, He teaches providing a command to grant decryption permission to others. (column 8 line 46 – column 9 line 37)

As per claim 58, He teaches the command to grant decryption permission includes:

GRANT DECRYPT ON table.column TO user_or_role_list

as its syntax. (column 8 line 46 – column 9 line 37)

As per claim 59, He teaches the database system internally stores in encrypted format any named encryption keys that have been created. (column 3 lines 37-57, column 8 lines 38-44)

As per claim 60, He teaches the database system stores encrypted column data internally as variable binary (VARBINARY) data. (column 5 lines 18-64)

As per claim 61, He teaches the database system presents users a user-defined field type for column data that has been encrypted, even though the column data is stored internally as variable binary data. (column 5 lines 18-64)

As per claim 62, He teaches the database system preserves any user-defined data type for the particular column data so that the database system employs a correct data type for processing queries and returning query results. (column 3 lines 17-57)

As per claim 63, He teaches the database system stores the user-defined data type for the particular column data in a system catalog of the database system. (column 3 lines 17-57)

As per claim 64, He teaches the particular named encryption key created comprises a symmetric encryption key. (column 5 lines 18-64)

As per claim 65, He teaches a single column named encryption key is used for each column to be encrypted. (column 6 lines 18-37)

As per claim 70, He teaches said Structured Query Language (SQL) extensions for creating and managing encryption keys include a clause for instructing the database system to create a default key for encrypting columns. (column 8 lines 2-24)

As per claim 71, He teaches "In a database system, a method for encrypting column data," (see Abstract)

"the method comprising: defining query language extensions for creating and managing column encryption keys, and for creating and managing database tables with encrypted column data; "(column 1 lines 60-67, column 3 lines 17-57, column 4 lines 1-57, wherein a security catalog is utilized by extended SQL syntax statements to access a secure database)

"in response to a first query language statement employing said extensions, creating a named encryption key for encrypting a particular column of a database table, said named encryption key being created with a syntactically unique name so that it can be referenced within other query language statements employing said extensions;" (column 6 line 39 – column 7 line 22, column 8 lines 2-44, wherein a public key can be created and employed by SQL statements)

"in response to a second query language statement employing said extensions, encrypting the particular column using said named encryption key, name including identifying said named encryption key upon parsing a portion of the statement that comprises the syntactically unique name for the key;" (column 5 lines 6-33, column 8 line 2 – column 9 line 17, wherein an SQL statement to encrypt columns of a database tables with an encryption key is received)

"and during a subsequent database operation requiring column data inserted to or selected from the particular column, automatically encrypting or decrypting the column data as necessary for carrying out the database operation." (column 7 line 42-7, column 8 lines 25-44, column 9 lines 13-37, wherein the column data can be dynamically encrypted ot decrypted based on key access, to be used in database operation)

As per claim 72, He teaches assigning privileges to users for creating an encryption key for encrypting column data. (column 3 lines 17-45, column 4 lines 1-56)

As per claim 73, He teaches in response to a request to create a named encryption key from a particular user, determining whether the particular user has sufficient privileges to create an encryption key. (column 7 lines 36-55)

As per claim 78, He teaches the database system stores encrypted column data internally as variable binary (VARBINARY) data. (column 5 lines 18-64)

As per claim 79, He teaches columns of the database table that are not specified to be encrypted are stored in unencrypted format. (column 5 lines 6-39)

As per claim 80, He teaches the system implements said extensions as SQL extensions for creating and managing named encryption keys and for creating and managing database tables with encrypted column data. (column 5 lines 6-33, column 8 lines 2-45

As per claim 81, He teaches said SQL extensions include a CREATE ENCRYPTION KEY command for creating a named encryption key. (column 6 line39 - column 7 line 55)

As per claim 82, He teaches said CREATE ENCRYPTION KEY command includes attributes specifying an encryption key name and a user-supplied password. (column 6 line 38 – column 7 line 22)

As per claim 83, He teaches said SQL extensions include a CREATE TABLE command having an attribute that allows specification of at least one column to be encrypted. (column 5 lines 6-38, column 8 lines 2-44)

As per claim 84, He teaches said CREATE TABLE command syntax includes attributes specifying a table name, one or more columns to be encrypted, and an encryption key name. (column 5 lines 6-38, column 8 lines 2-44)

As per claim 85, He teaches said second query language statement includes a request specifying alteration of a previously-created table so as to encrypt particular column data. (column 5 lines 32-64)

As per claim 86, He teaches a user subsequently requiring use of the encrypted column data must provide a user-supplied password for unlocking the named encryption key for the particular column. (column 6 line 38 – column 7 line 22)

As per claim 87, He teaches receiving a query language statement specifying creation of a default key encryption password. (column 8 lines 2-24)

As per claim 88, He teaches the query language statement specifying creation of a default key encryption password specifies a default password value that is encrypted by a system stored procedure, for storage in a system table of a particular database. (column 8 lines 2-24)

As per claim 89, He teaches receiving a query language statement specifying creation of an encryption keypair. (column 5 lines 6-64)

As per claim 90, He teaches the query language statement specifying creation of an encryption keypair comprises a CREATE ENCRYPTION KEYPAIR command. (column 8 lines 2-44)

As per claim 91, He teaches the CREATE ENCRYPTION KEYPAIR command includes:

CREATE ENCRYPTION KEYPAIR keypairname
[FOR algorithm]
[WITH [KEYLENGTH keysize]
[PASSWD passphrase | LOGIN_PASSWD]

as its syntax. (column 8 lines 2-44)

As per claim 92, He teaches receiving a query language statement specifying alteration of a particular named encryption key or keypair. (column 5 lines 32-64)

As per claim 93, He teaches receiving a query language statement specifying dropping a particular named encryption key or keypair. (column 5 lines 32-64)

As per claim 94, He teaches receiving a query language statement granting rights to a particular named encryption key or keypair. (column 8 line 46 – column 9 line 37)

As per claim 95, He teaches receiving a query language statement revoking said rights that have been granted to a particular named encryption key or keypair. (column 8 line 46 – column 9 line 37)

As per claim 96, He teaches said rights granted for the particular named encryption key or keypair comprise SELECT query execution rights, for selecting encrypted data. (column 9 lines 6-37)

As per claim 97, He teaches said rights granted for the particular named encryption key or keypair comprise ALTER query execution rights, for altering the encryption key or keypair. (column 9 lines 6-37)

As per claim 98, He teaches A computer-readable medium having processor-executable instructions for performing the method of claim 71. (column 2 lines 13-24)

As per claim 99, He teaches A downloadable set of processor-executable instructions for performing the method of claim 71. (column 2 lines 13-24)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 32-35, 66-69, and 74-77 are rejected under 35 U.S.C. 103(a) as being anticipated by He et al. (US Patent 7,269,729 B2) in view of Newman et a. US Patent 7,266,699 B2)

As per claim 32, He is taught as per claim 1 above. He additionally teaches user supplied passwords utilized to create encryption keys (column 6 line 39 - column 7 line 27). He does not specifically teach named encryption key is itself encrypted by a key-encrypting key constructed from a user-supplied password.

Newman teaches a named encryption key is itself encrypted by a key-encrypting key constructed from a user-supplied password. (column 5 lines 13-30, column 6 lines 11—column 7 line 4, wherein an encryption key is itself encrypted by another encrypting key from a user password)

It would have been obvious at the time the invention was made for one of ordinary skill in the art to combine He's method of internally encrypting column data in a

database based on encryption keys with Newman's ability to further encrypt the encryption keys utilized in a method to encrypt data. This gives the user the advantage of added security to prevent unauthorized access to the data. The motivation for doing so would be to allow multiple user access to files for encryption and decryption (column 1 lines 33-45)

As per claim 33, Newman teaches the named encryption key is itself stored on disk in encrypted format using Advanced Encryption Standard (AES) encryption. (column 4 lines 19-28, column 5 lines 31-37)

As per claim 34, Newman teaches the user-supplied password may comprise a hex literal. (column 10 lines 8-18)

As per claim 35, Newman teaches the user-supplied password is itself transformed into a symmetric encryption key, using a random salt, internal static data, and SHA-1 hashing algorithm. (column 4 lines 19-28, column 10 lines 30-62)

As per claim 66, He is taught as per claim 37 above. He additionally teaches user supplied passwords utilized to create encryption keys (column 6 line 39 - column 7 line 27). He does not specifically teach named encryption key is itself encrypted by a key-encrypting key constructed from a user-supplied password.

Newman teaches a particular named encryption key is itself encrypted by a key-encrypting key constructed from a user-supplied password. (column 5 lines 13-30, column 6 lines 11—column 7 line 4, wherein an encryption key is itself encrypted by another encrypting key from a user password)

It would have been obvious at the time the invention was made for one of ordinary skill in the art to combine He's method of internally encrypting column data in a database based on encryption keys with Newman's ability to further encrypt the encryption keys utilized in a method to encrypt data. This gives the user the advantage of added security to prevent unauthorized access to the data. The motivation for doing so would be to allow multiple user access to files for encryption and decryption (column 1 lines 33-45)

As per claim 67, Newman teaches the particular named column encryption key is itself stored on disk in encrypted format using Advanced Encryption Standard (AES) encryption. (column 4 lines 19-28, column 5 lines 31-37)

As per claim 68, Newman teaches the user-supplied password may comprise a hex literal. (column 10 lines 8-18)

As per claim 69, Newman teaches the user-supplied password is itself transformed into a symmetric encryption key, using a random salt, static internal data and SHA-1 hashing algorithm. (column 4 lines 19-28, column 10 lines 30-62)

As per claim 74, He is taught as per claim 71 above. He additionally teaches user supplied passwords utilized to create encryption keys (column 6 line 39 - column 7 line 27). He does not specifically teach a named encryption key is itself encrypted by a key-encrypting key constructed from a user-supplied password.

Newman teaches a named encryption key is itself encrypted by a key-encrypting key constructed from a user-supplied password. (column 5 lines 13-30, column 6 lines

11—column 7 line 4, wherein an encryption key is itself encrypted by another encrypting key from a user password)

It would have been obvious at the time the invention was made for one of ordinary skill in the art to combine He's method of internally encrypting column data in a database based on encryption keys with Newman's ability to further encrypt the encryption keys utilized in a method to encrypt data. This gives the user the advantage of added security to prevent unauthorized access to the data. The motivation for doing so would be to allow multiple user access to files for encryption and decryption (column 1 lines 33-45)

As per claim 75, Newman teaches the named encryption key is encrypted using Advanced Encryption Standard (AES) encryption. (column 4 lines 19-28, column 5 lines 31-37)

As per claim 76, Newman teaches the user-supplied password may comprise a hex literal. (column 10 lines 8-18)

As per claim 77, Newman teaches the user-supplied password is itself transformed into a symmetric encryption key, using a random salt, static internal data and SHA-1 hashing algorithm. (column 4 lines 19-28, column 10 lines 30-62)

Response to Arguments

7. Applicant's arguments with respect to the 35 USC 103(a) rejection of claims 1-99 have been considered but are moot in view of new grounds of rejections. The newly cited prior art of He discloses the limitations of independent claims 1, 37, and 71. In

particular, He teaches creating uniquely identified encryption keys to be utilized in database operations (column 6 line 39 – column 7 line 55).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Rothwein et al. (US Patent 6,233,617 B1)

Matsuzaki et al. (US Publication 2001/0056541 A1)

Jaganathan et al. (US Publication 2005/0198490 A1)

Licis (US Patent 7,155,612 B2)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANGELINO N. GORTAYO whose telephone number is (571)272-7204. The examiner can normally be reached on M-F 7:30-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim T. Vo can be reached on (571)272-3642. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dangelino N Gortayo/
Examiner, Art Unit 2168

/Tim T. Vo/
Supervisory Patent Examiner, Art Unit 2168

Dangelino N. Gortayo
Examiner

Tim T. Vo
SPE